BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

MEMORANDUM NO. M-2012-_017_

To : **ALL BSP COVERED INSTITUTIONS**

Subject : **ANTI-MONEY LAUNDERING RISK RATING SYSTEM (ARRS)**

The Monetary Board, in its Resolution No.362 dated 2 March 2012, approved to adopt the attached ARRS to be employed by BSP in the conduct of on-site examination. It is broken into the following parts:

1. ARRS OVERVIEW which introduces the system and provides for a background and general information on how it works;
2. ANNEX A- Composite Ratings Table
3. COMPONENT I- Efficient Management Component Rating
4. COMPONENT II- Sound MLPP Component Rating
5. COMPONENT III- Robust Internal Audit and Control
6. COMPONENT IV- Effective Implementation
7. ANNEX B- Details of the Factors to be considered in assessing Effectivity of Implementation
8. ANNEX B.1- Survey Questionnaire
9. ANNEX C- Monetary Penalty Guidelines

In this connection, BSP covered institutions are expected to comprehend the ARRS and give their utmost cooperation in the implementation of this Rating System.

For information and guidance.

AMANDO M. TETANGCO, JR.
Governor

_4_ April 2012

Att: A/S

BANGKO SENTRAL NG PILIPINAS

BSP ANTI-MONEY LAUNDERING RISK RATING SYSTEM OVERVIEW

Background

The Congress of the Philippines enacted Republic Act (R. A.) No. 9160, otherwise known as the Anti-Money Laundering Act of 2001 (AMLA), to prevent banks, insurance companies, securities brokers and other financial service providers that are supervised and regulated by Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), and Insurance Commission (IC) from being used as a money laundering conduit for the proceeds of specified unlawful activities. The law was later on amended by R. A. No. 9194 and the Revised Implementing Rules and Regulations (RIRR) was later approved by the Congressional Oversight Committee. These are the tools the Philippine Government uses to combat money laundering.

One of the amendments introduced by R. A. No. 9194 is a provision (Section 11) that mandates BSP "to ensure compliance with the AMLA, as amended" and at the same time vests it with authority to "inquire into or examine any deposit or investment with any banking institution or non-bank financial institution when the examination is made in the course of a periodic or special examination, in accordance with the rules of examination of the BSP." It is the Supervision and Examination Sector (SES) of the BSP that executes this mandate and authority. In the course of periodic or special examination, SES monitors compliance with AMLA, as amended, and its RIRR by Banks and Non-Bank Financial Institutions under its supervision and regulation.

However, with BSP's adoption of a full risk based approach to supervision, it is essential that the AML rules and regulations are likewise geared toward risk-based principles. For this reason and in accordance with Rule 17.1 (b) of the RIRR authorizing supervising authorities such as the BSP to issue, under its Charter and regulatory authority, guidelines and circulars on AML to effectively implement the provisions of the AMLA, as amended, the Monetary Board, in its Resolution No. 1801 dated 16 December 2010, approved the adoption of the Updated Anti-Money Laundering Rules and Regulations (UARR). The same Monetary Board Resolution authorized the Governor to issue the corresponding Circular. Hence, Circular No. 706 dated 5 January 2011 was issued, published in a newspaper of general circulation on 12 January 2011, and took effect on 27 January 2011.

Introduction

A necessary consequence of a risk-based approach to supervision is the development of a risk-focused examination process that is complemented by the adoption of an Anti-Money Laundering (AML) risk rating system. This is not intended to add to the regulatory burden of BSP covered institutions or require additional policies or processes. Rather it is consistent with Principle 19 of the Basel Core Principles of Effective Banking Supervision which encourages Supervisors to develop and maintain a thorough understanding of the operations of individual banks, banking groups and the banking system as a whole.

The AML risk rating system is an internal rating system to be used by BSP to understand whether the risk management policies and practices as well as internal controls of Banks and Non-Bank Financial Institutions to prevent money laundering and terrorist financing are in place, well disseminated and effectively implemented. In doing so to individual banks, BSP will have an over-all understanding of the whole banking system's risk management policies and practices as well as internal controls relative to money laundering and terrorist financing prevention.

This AML risk rating system is an effective supervisory tool that undertakes to ensure that all covered institutions as defined under Circular No. 706 are assessed in a comprehensive and uniform manner, and that supervisory attention is appropriately focused on entities exhibiting inefficiencies in Board of Directors and Senior Management oversight and monitoring, inadequacies in their AML framework, weaknesses in internal controls and audit and defective implementation of internal policies and procedures.

Overview of the Rating System

Under the AML Risk Rating System, each covered institution is assigned a Composite Rating based on an assessment of four (4) components of a covered institution's framework and operations in the prevention of money laundering (ML) and terrorist financing (TF). These component factors address the following:

1. Efficient Board of Directors (BOD) and Senior Management (SM) oversight ("Management");
2. Sound AML policies and procedures embodied in a Money Laundering and Terrorist Financing Prevention Program duly approved by the Board of Directors ("MLPP");
3. Robust internal controls and audit ("Controls and audit"); and
4. Effective implementation ("Implementation").

Evaluation of the components takes into consideration the covered institution's responses to various questions that are designed to comprehend its business operations as well as its risk profile. The responses will be assessed and on-site examination will confirm their veracity and accuracy. Thereafter, a Component Rating will be assigned to reflect whether or not the covered institution possesses any or all of the component factors stated above based on the combined results of the off-site evaluation of replies to the questionnaire and on-site confirmation of their veracity and accuracy. In case the veracity and accuracy of the written responses could not be confirmed, the examiner shall determine whether or not to accept as accurate the written responses submitted by the covered institution. The component ratings to be assigned ranging from 4 as the highest and 1 as the lowest are discussed in every component factor.

The Composite Rating generally bears a close relationship to the Component Ratings assigned. However, the Composite Rating is not derived by computing an arithmetic average of the Component Ratings. Each Component Rating is based on a qualitative analysis of that component and its interrelationship with the other components. The

Composite Rating is assigned based on a 1 to 4 numerical scale. The highest rating of 4 indicates the strongest risk management system and most effective operational practices that entail the least degree of supervisory concern. The lowest rating of 1 on the other hand signifies the weakest risk management system and defective implementation which requires the highest degree of supervisory concern including the placement of the covered institution within the framework of prompt corrective action.

The assigned Composite and Component Ratings are disclosed to the covered institution's board of directors and senior management together with an indication of its level of compliance with AMLA, as amended, its RIRR and Circular No. 706.

Composite Ratings (See Table in Annex A)

The Composite Ratings are defined as follows:

Composite 4

The level of over-all money laundering and terrorist financing prevention risk management and control framework relative to the size, complexity, and risk profile is high and without cause for supervisory concern. The risk and control framework is clearly defined and fully compatible with the nature and complexity of the institution's activities. All or most of its component ratings are 4 with no component rating below 3. It is most capable of withstanding any risk associated with money-laundering and is unlikely to be used as a money laundering conduit for the proceeds of unlawful activities.

Composite 3

The level of over-all money laundering and terrorist financing prevention risk management and control framework relative to the size, complexity, and risk profile is acceptable and with minimal supervisory concern. The risk management and control framework is adequately defined and sufficiently compatible with the nature and complexity of the institution's activities. All or most of its component ratings are 3 with no component rating below 2. It can withstand any associated AML risks and are there's low probability of it being used as a money laundering conduit for the proceeds of unlawful activities.

Composite 2

The level of over-all money laundering and terrorist financing prevention risk management and control framework relative to the size, complexity, and risk profile needs improvement and requires more than normal supervision. Risks are insufficiently controlled and mitigated, leaving too high a residual risk for the institution. The risk management and control framework is poorly defined or insufficiently compatible with the nature and complexity of the institution's activities. All or most of its component

ratings are 2. It is vulnerable to AML risks and may be used as a money laundering conduit for the proceeds of unlawful activities.

Composite 1

The level of over-all money laundering and terrorist financing prevention risk management and control framework relative to the size, complexity, and risk profile need drastic and/or immediate improvement and requires close supervisory attention. Risks are not or inadequately mitigated and poorly controlled. The risk management and control framework is neither defined nor compatible with the nature and complexity of the institution's activities. All or most of its component ratings are 1. It is not capable of withstanding AML risks and may likely be used as a conduit for the proceeds of unlawful activities.

Component Ratings

Each of the Component Rating descriptions is discussed separately on each component factor.

Survey questionnaire shown in **Annex B.1** will be given to covered institutions during visitation and shall be answered by the Compliance Officer or a duly authorized officer, which will be subject to confirmation during onsite examination.

Enforcement Actions under Circular No. 706

Section X811 of Circular No. 706 provides for the basis of enforcement actions, *to wit:*

> ***"Section X811. Sanctions and Penalties.*** *In line with the objective of ensuring that covered institutions maintain high anti-money laundering standards in order to protect its safety and soundness as well as protecting the integrity of the national banking and financial system, violation of these Rules shall constitute a major violation subject to the following enforcement actions against the Board of Directors, Senior Management and line officers, not necessarily according to priority:*
>
> *1. Written reprimand;*
>
> *2. Suspension or removal from the office they are currently holding; and/or*
>
> *3. Disqualification from holding any position in any covered institution.*

"In addition to the non-monetary sanctions stated above, BSP may also impose monetary penalties computed in accordance with existing regulations and in coordination with the Anti-Money Laundering Council.

"Enforcement actions shall be imposed on the basis of the over-all assessment of the covered institution's AML risk management system. Whenever a covered institution's AML compliance system is found to be grossly inadequate, this may be considered as unsafe and unsound banking practice that may warrant initiation of prompt corrective action."

To implement the enforcement action provisions of Circular No. 706 along with the AML risk rating system, the following rules shall apply:

1. An AML Composite rating of 4 and 3 will require no enforcement action.

2. An AML composite rating of 2 and 1 will require submission by the covered institution to the AMLSG, SES, of a written action plan duly approved by the BOD aimed at correcting the noted inefficiency in BOD and SM oversight, inadequacy in AML and TF policies and procedures, weakness in internal controls and audit, and/or ineffective implementation within a reasonable period of time.

   The AMLSG shall assess the viability of the plan and shall monitor the covered institution's performance.

   In the event of non-submission of an acceptable plan within the deadline or failure to implement its action plan, AMLSG shall recommend appropriate enforcement actions on the covered institution and its responsible officers including monetary penalties to be computed on a daily basis until improvements are satisfactorily implemented.

3. An AML rating of 1 shall also be considered as an unsafe and unsound banking practice. For this reason, prompt corrective action shall also be automatically initiated on the covered institution.

ANNEX A

ANTI-MONEY LAUNDERING (AML) RATING SYSTEM
Composite Ratings

Composite Rating				
Numerical Rating	**4**	**3**	**2**	**1**
Adjectival Rating	Sound.	Adequately Sound.	Vulnerable.	Grossly Inadequate.
Over-all Money Laundering (ML) and Terrorist Financing (TF) Prevention Risk Management Framework ***(relative to size, complexity and risk profile)***	High level of risk management and control without cause for supervisory concern. The risk and control framework is clearly defined and fully compatible with the nature and complexity of the institution's activities.	Acceptable level of risk management and control with minimal supervisory concern. The risk management and control framework is adequately defined and sufficiently compatible with the nature and complexity of the institution's activities.	Risk Management and Control needs improvement and requires more than normal supervision. Risks are insufficiently controlled and mitigated, leaving too high a residual risk for the institution. The risk management and control framework is poorly defined or insufficiently compatible with the nature and complexity of the institution's activities.	Risk management needs drastic and/or immediate improvement which requires close supervisory attention. Risks are not or inadequately mitigated and poorly controlled. The risk management and control framework is neither defined nor compatible with the nature and complexity of the institution's activities.
Components[1] Rating	All or mostly 4 with no component rating less than 3	All or mostly 3 but no component rating less than 2	All or mostly 2	All or mostly 1
Capacity to Withstand AML Risks	Most capable of withstanding AML risks and is unlikely to be used as money laundering conduit for the proceeds of unlawful activities.	Can withstand any associated AML risks and there is low probability of it being used as a money laundering conduit for the proceeds of unlawful activities.	Vulnerable to AML risks and may be used as money laundering conduit for the proceeds of unlawful activities.	Not capable of withstanding AML risks and may likely be used as a conduit for the proceeds of unlawful activities.
Enforcement Actions and/or Monetary Penalties	None	None	Warning to written reprimand. Monetary penalties may be imposed on a one-time basis.	Warning, written reprimand or suspension. Monetary penalties may be imposed computed from date of notice until the improvement is satisfactorily effected.

[1] *Consist of (i) Efficient BOD and SM Oversight ("Management"); (ii) Sound AML policies and procedures embodied in a Money Laundering and Terrorist Financing Prevention Program duly approved by the BOD ("MLPPP"); (iii) robust internal controls and audit ("internal controls and audit"); and (iv) effective implementation*

COMPONENT I

EFFICIENT MANAGEMENT COMPONENT RATING

I. DESCRIPTION

The management rating reflects the efficiency and capability of the BOD and SM oversight to identify, measure, monitor and control money laundering risks inherent in the covered institution's activities. It is recognized, however, that appropriate risk management practices vary considerably among financial institutions, depending on its size, complexity and risk profile.

The BOD shall be ultimately responsible in ensuring that the covered institution strictly comply with the requirements under Circular No. 706 ("UARR"), the AMLA and its RIRR through adoption of an appropriate ML and TF prevention framework appropriate to the institution's corporate structure, operations and risk profile, which shall be embodied in its BOD-approved Money Laundering and Terrorist Financing Prevention Program (MLPP). The BOD may also delegate other duties and responsibilities to SM and/or committees created for the purpose but not the ability to oversee the institution's compliance with UARR, the AMLA and its RIRR. The Compliance Officer shall be responsible for effectively managing the implementation of the MLPP, specifically its ML and TF prevention practices and procedures. The delegated authorities, together with the standards, internal control measures, risk tolerance levels should also be embodied in the MLPP. This will facilitate the resolution of some or all of the following risks: (i) reputational[1]; (ii) operational[2]; (iii) legal[3]; and (iv) concentration[4].

Assessment of the over-all efficiency of Board of Director's and Senior Management's oversight in relation to the size, complexity and risk profile of the covered institution takes into account the following characteristics:

1. Ability of the Compliance Office to manage the MLPP;
2. Reliability, timeliness, completeness and helpfulness of management information system;
3. Consistent and effective identification, measurement, monitoring and controlling of risks and problems related to ML and TF (risk management practices); and
4. Independence, accuracy and usefulness of self assessment systems that are either proactive (through compliance testing), or reactive (through internal audit).

---

[1] ***Reputation risk*** *refers to the potential that an adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.*

[2] ***Operational risk*** *is defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and system or from external events.*

[3] ***Legal risk*** *is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or conditions of a bank.*

[4] ***Concentration risk*** *is a supervisory concern as it mostly applies on the asset side of the balance sheet. On the liabilities side, concentration risk is closely associated with funding risk or the risk of early or sudden withdrawal of funds by large depositors with potentially damaging consequences to bank's liquidity.*

II. RATINGS

Component Rating ("Management")				
Numerical Rating	**4**	**3**	**2**	**1**
Over-all efficiency of the BOD and SM oversight relative to the size, complexity and risk profile	Strong and efficient oversight	Adequate oversight	Less than adequate	Weak oversight
Sub-components rating	All or mostly 4 with no sub-component rating less than 3	All or mostly 3 but no sub-component rating less than 2	All or mostly 2	All or mostly 1
SUB-COMPONENTS RATING				
Numerical Rating	**4**	**3**	**2**	**1**
1. Ability of the Compliance Office to manage the MLPP	High level ability to manage the MLPP resulting to minor violations/ findings	Acceptable level of ability to manage the MLPP, resulting to minimal violations/ findings	Less than acceptable ability to manage the MLPP, resulting to moderate violations/ findings	Low ability to manage the MLPP resulting to excessive violations/ findings
2. Management Information System (MIS) (Reliable, timely, complete and helpful)	High level MIS that are reliable, timely, complete and helpful	Satisfactorily reliable, timely, complete and helpful MIS	Less than satisfactorily reliable, timely, complete and helpful MIS	Low level of reliability, timeliness, completeness and helpfulness of MIS
3. Risk Management Practices related to ML and TF prevention (consistent and effective)	High level risk management practice that consistently and effectively identifies, measures monitors and controls risks and problems	Satisfactorily identifies, measures monitors and controls risks and problems relative to ML and TF	Less than satisfactorily identifies, measures monitors and controls risks and problems	Low level risk management practice
4. Pro-active or reactive Self-assessment systems (Independent, accurate and useful)	High level self-assessment system that are independent, accurate and useful	Adequately independent, accurate and useful self-assessment systems	Less than adequately independent, accurate and useful self-assessment systems	Low level self-assessment system

COMPONENT II

SOUND MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM (MLPP) COMPONENT RATING

I. DESCRIPTION

This rating reflects the adequacy of appropriate policies and procedures in preventing money laundering and terrorist financing as approved by the covered institution's BOD and cascaded to all concerned (i.e. SM, Compliance Office and across all departments etc.).

Assessment of the soundness of ML and TF prevention policies and procedures includes the adoption of a comprehensive and risk-based MLPP. It is understood though that covered institutions shall have a degree of flexibility in implementing policies and procedures which corresponds to their own risk assessment. However, there are minimum legal and regulatory requirements and elements that apply regardless of the risk level as provided under AMLA, its RIRR and IARR. Moreover, the MLPP should at least have the following features:

1. It shall be consistent with the provisions set out in the UARR and designed according to the covered institution's corporate structure, risk profile and complexity;
2. It shall be in writing (duly approved by its BOD or by its country/regional head or its equivalent for local branches of foreign banks and institution-wide covering all the institution's branches and offices and its subsidiaries and affiliates, whether within or outside the Philippines) and well disseminated to all officers and staff who are obliged by law or by their program to implement the same;
3. It shall also be readily available in user-friendly form, whether in hard or softcopy.
4. It shall be periodically updated to incorporate new AML issuances, changes in the institution's corporate structure and risk profile, and development of products and innovations;
5. The covered institution must put up a procedure to ensure that an audit trail evidences the dissemination process for new and amended policies and procedures;
6. The program shall embody the following **at a minimum**:
   a. Detailed procedures of the covered institution's compliance and implementation of the following major requirements of the AMLA, its RIRR and these rules on the following:
      a.1. Customer identification and acceptance;
      a.2. Recordkeeping;
      a.3. Covered transaction reporting; and
      a.4. Suspicious transaction reporting;
   b. Continuous training policies on employees (i.e newly-hired, directors, officers etc.), which may include refresher trainings and intermittent post-training tests;
   c. Adequate screening and recruitment process;
   d. Independent audit function with written scope of audit, audit program as well as policies and procedures;

e. A system that will ensure that deficiencies noted during the audit and/or BSP regular or special examination are immediately corrected and acted upon;
f. Cooperation with the AMLC and its Secretariat and to other relevant authorities; and
g. Designation of an AML Compliance Officer[1] at managerial level as the lead during the implementation of the program within an adequately staffed compliance office.

II. RATING

Component Rating ("MLPP")				
Numerical Rating	**4**	**3**	**2**	**1**
Overall assessment of MLPP in relation to CI's corporate structure, complexity and risk profile	Sound and appropriate to its corporate structure, complexity and risk profile	Satisfactory and proper to its corporate structure, complexity and risk profile	Less than satisfactory and does not fully support its corporate structure, complexity and risk profile	Deficient
Sub-components rating	All or mostly 4 with no sub-component rating less than 3	All or mostly 3 but no sub-component rating less than 2	All or mostly 2	All or mostly 1
SUB-COMPONENTS RATING				
Numerical Rating	**4**	**3**	**2**	**1**
1. Coverage of MLPP *(as to AMLA, RIRR and Circular No. 706)*	Comprehensively covers all regulatory requirements	Significantly covers all regulatory requirements	Needs improvement as it lacks some major provisions	Deficient as majority of the provisions are not indicated
2. Risk Management Practices related to ML and TF are incorporated in the MLPP	All significant risks are identified and practices to monitor and control these risks are incorporated in the MLPP	Most significant risks are identified and practices to monitor and control these risks are adequately incorporated in the MLPP	Risks may be identified but practices to monitor and control these risks are inadequately incorporated in the MLPP	Deficient risk management practices where risks are not identified and practices and procedures are not available
3. Extent of dissemination of MLPP and level of awareness	Well disseminated to all concerned officers/staff, resulting to full awareness of their respective duties and responsibilities	Disseminated to most of the concerned officers/staff, resulting to reasonable awareness of their duties and responsibilities	Disseminated only to some of the concerned officers/staff, where level of awareness needs improvement	Poor dissemination to concerned officers/staff and awareness of their duties and responsibilities

[1] *The AML compliance officer may be liaison between the covered institution, the BSP and the AMLC in matters relating to compliance. Where resources of the covered institution do not permit the hiring of an AML compliance officer, the present Compliance Officer shall assume the responsibility.*

COMPONENT III

ROBUST INTERNAL CONTROL AND AUDIT COMPONENT RATING

I. DESCRIPTION

This component rates the adequacy and soundness of the internal controls of the covered institution to identify, measure, monitor and control money laundering risks as well as compliance with AMLA, its RIRR and BSP rules and regulations. There should be an internal audit unit that is independent and directly reporting to the BOD or audit committee. Generally, an internal audit report can be used as reference to assess the performance of the internal control and audit function.

The internal control and audit rating is based upon, but not limited to the assessment of the following:

1. Internal Controls
   a. The framework of internal controls should, at a minimum, contain the following:
      a.1. Adequate board and senior management oversight;
      a.2. Appropriate policies and procedures
      a.3. Adequate measurement and monitoring system;
      a.4. Effective internal controls and audit; and
      a.5. Continuing personnel development and training
   b. Other AML controls shall be evaluated based on the following:
      b.1. Nature, scale and complexity of the institution's business;
      b.2. Diversity of the institution's operations, including geographical diversity;
      b.3. Institution's customer, product and activity profile;
      b.4. Volume and size of the transactions;
      b.5. Degree of risk associated with each area of the institution's operation;
      b.6. Extent to which the institution is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non face-to-face access.

2. Audit Function
   a. Assessment by the internal audit unit of the institution's compliance and adequacy with the AMLA and with internally established policies and procedures shall be based on the following:
      a.1. Status;
      a.2. Policies and procedures;
      a.3. Control environment; and
      a.4. Manpower complement of the internal audit department
   b. The institution's internal auditor should be able to:
      b.1. Attest to the overall integrity and effectiveness of management systems and controls and AMLA compliance;

b.2. Test transactions in all areas of the institution with emphasis on high risk areas, products and services;

b.3. Assess the following:

i. Employee's knowledge and regulations/procedures;

ii. Adequacy, accuracy and completeness of training programs; and

iii. Adequacy of the institution's process for identifying suspicious activity

Ratings

Composite Rating ("Internal Control and Audit")				
Numerical Rating	**4**	**3**	**2**	**1**
Over-all assessment of Internal Controls and Audit for ML and TF prevention	Robust	Satisfactory	Less than satisfactory	Deficient
Sub-components rating	All or mostly 4 with no sub-component rating less than 3	All or mostly 3 but no sub-component rating less than 2	All or mostly 2	All or mostly 1
SUB-COMPONENTS RATING				
Numerical Rating	**4**	**3**	**2**	**1**
1. Independence and support	Fully independent and has total support of BOD and SM	Satisfactorily independent and has sufficient support from BOD and SM	Less than satisfactory independence and/or support from the BOD and SM	Lacks independence and/or support from the BOD and SM
2. Coverage	Comprehensively covers all areas of concern	Significantly covers all areas of concern	Needs improvement as it fails to cover some major concerns	Deficient as majority of the areas of concern were not covered
3. Timeliness of communication of Internal Audit Reports	Prompt communication to the BOD and Compliance Office, and corrective actions are immediately taken	Communication to BOD and Compliance Office and corrective actions are within reasonable time	Communication to BOD and Compliance Office and corrective actions need improvement	Poor communication to the BOD and Compliance Office resulting to delayed corrective actions

COMPONENT IV

EFFECTIVE IMPLEMENTATION

I. DESCRIPTION

Establishment of a comprehensive and risk-based ML and TF framework embodied in the MLPP as well as internal controls and audit system proved to be futile if not effectively implemented by SM, resulting to untimely and irrelevant information to the BOD to act on. Thus, it is equally important to assess the effectivity of its implementation. Assessment shall take into account the implementation of the following policies and procedures on (details on **Annex B**):

1. Risk-based and tiered customer acceptance and identification;
2. On-going monitoring of transactions through an effective electronic (UBs/KBs) or manual AML system that are capable of watch list monitoring, initiating investigation, providing a complete audit trail and aggregating activities of a customer with multiple accounts;
3. Covered Transaction Reporting system either electronic (UBs/KBs) or manual that is capable of performing statistical analysis, profiling and detecting unusual patterns of account activity, and accurately and completely generating all covered transaction reports with all mandatory fields properly filled up;
4. Suspicious Transaction Reporting system either electronic (UBs/KBs) or manual that is capable of performing statistical analysis, profiling and detecting unusual patterns of account activity, and recording all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC;
5. Recordkeeping and retention system; and
6. Continuing education and training program.

II. RATINGS

Component Rating ("Implementation")				
Numerical Rating	**4**	**3**	**2**	**1**
Overall assessment of Implementation	High level of effectiveness	Acceptable level of effectiveness	Implementation needs improvement	Poor implementation
Sub-components rating	All or mostly 4 with no sub-component rating less than 3	All or mostly 3 but no sub-component rating less than 2	All or mostly 2	All or mostly 1
SUB-COMPONENTS RATING				
Numerical Rating	**4**	**3**	**2**	**1**
1. Assessment of risk-based and tiered customer acceptance and identification	Sound risk-based and tiered customer acceptance and identification	Adequate risk-based and tiered customer acceptance and identification	Risk-based and tiered customer acceptance and identification needs improvement	Deficient risk-based and tiered customer acceptance and identification

COMPONENT IV

2. On-going monitoring of transactions and activities of customers	Robust electronic or manual AML monitoring system of transactions and activities of customers	Acceptable AML monitoring system of transactions and activities of customers	AML monitoring system of transactions and activities of customers needs improvement	Deficient AML monitoring system of transactions and activities of customers
3. Assessment of covered transaction reporting system	Sound covered transactions reporting system	Satisfactory covered transactions reporting system	Less than satisfactory covered transactions reporting system	Poor covered transactions reporting system
4. Assessment of suspicious transaction reporting system	Sound suspicious transactions reporting system	Satisfactory suspicious transactions reporting system	Less than satisfactory suspicious transactions reporting system	Poor suspicious transactions reporting system
5. Assessment of record keeping and retention system	High level of effectiveness in record keeping and retention system	Adequate level of effectiveness in record keeping and retention system	Record keeping and retention system needs improvement	Poor record keeping and retention system
6. Assessment of continuing education and training program	High level effectiveness of continuing education and training program	Adequate level effectiveness of continuing education and training program	Continuing education and training program needs improvement	Weak continuing education and training program

ANNEX B

DETAILS OF THE FACTORS TO BE CONSIDERED IN ASSESSING EFFECTIVITY OF IMPLEMENTATION

1. Risk based and tiered customer acceptance, identification and on-going monitoring policies and procedures

The assessment shall be based upon, but not limited to, an assessment of the following factors:

a. Existence of a clear, written and graduated acceptance policies and procedures specifying the criteria and description of the types of customers who are likely to pose low, normal, or high risk as well as the standards in applying reduced, average and enhanced due diligence including a set of conditions for the denial of account opening and how are these implemented and monitored.

b. System of validating information for customers that pose high risk to its operations are religiously implemented and monitored.

c. Identification customers that pose low risk to its operations and the criteria are clearly stated, executed and monitored.

d. Existence of mechanisms related to outsourcing arrangement of face-to-face and obtaining of KYC information and/or documents as well as third party reliance are adopted and carefully scrutinized.

e. Determination of the completeness of the following minimum KYC information/documents required to be obtained from customers:

- For Individual Customers (must be obtained within reasonable period after establishing business relationship)

1) Name;
2) Present address;
3) Date and place of birth;
4) Nature of work, name of employer or nature of self-employment/business;
5) Contact details;
6) Specimen signature;
7) Source of funds.
8) Permanent address;
9) Nationality;
10) Tax identification number, Social Security System number or Government Service Insurance Number, if any; and

11) Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, whenever applicable.

- For Corporate and other Juridical Entities (must be obtained before establishing business relationship)

1) Certificates of Registration issued by the Department of Trade and Industry for single proprietors, or by the Securities and Exchange Commission, for corporations and partnerships, and by the BSP, for money changers/foreign exchange dealers and remittance agents;
2) Articles of Incorporation or Association and By-Laws;
3) Principal business address;
4) Board or Partners' Resolution duly certified by the Corporate/Partners' Secretary authorizing the signatory to sign on behalf of the entity;
5) Latest General Information Sheet which lists the names of directors/trustees/partners, principal stockholders owning at least twenty percent (20%) of the outstanding capital stock and primary officers such as the President and Treasurer;
6) Contact numbers of the entity and authorized signatory/ies;
7) Source of funds and nature of business;
8) Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, if applicable; and
9) For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by the Philippine Consulate where said entities are registered.

f. Assessment of the detailed description of policies and procedures for accepting and monitoring of the following customers:

1) Private banking/ wealth management customers;
2) Politically exposed persons;
3) Correspondent banking partners;
4) Wire transfer clients;
5) Buyers of Cashier's, Manager's or Certified Checks;
6) Depositors of second endorsed checks;
7) Foreign exchange dealers, money changers and remittance agents;
8) High risk customers as defined by its MLPP;
9) Shell Company/ Shell Banks;
10) Numbered account holders;
11) Accounts with fictitious or anonymous names;
12) Trustee, nominee and agent accounts;
13) Custodianship arrangement customers;
14) Other types of customers

g. Conduct of internal assessment through sample testing and internal audit of covered institution's processes in customer acceptance including policies on the conduct of face-to-face contact, identification, documentation and on-going monitoring

2. Covered (CT) and Suspicious Transaction (ST) Reporting Policies and Procedures

The reporting requirement of a covered institution is rated based upon, but not limited to, an assessment of the following factors:

a. For UBs and KBs, the covered institution has established an electronic money laundering transaction monitoring system which at the minimum shall detect and raise to the covered institution's attention, transactions and/or accounts that qualify either as covered or suspicious transactions. The AML electronic system shall have, at least, the following automated functionalities:

   1) Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
   2) Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
   3) Investigation – checks for given names throughout the history of payment stored in the system;
   4) Can generate all the CTRs of the covered institution accurately and completely with all the mandatory field properly filled up;
   5) Must provide a complete audit trail;
   6) Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
   7) Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC.

b. For covered institution other than UBs and KBs, it has means of flagging and monitoring the transactions mentioned above.

c. The covered institution's CT and ST reporting system is pro-actively evaluated through compliance testing by the Compliance Office and reviewed by the Internal Audit to ensure that CTs and STs are:

   1) Timely submitted to the AMLC within ten (10) working days from occurrence thereof;
   2) Completely submitted to the AMLC; and
   3) Accurately reported in accordance with the manner, form and procedures prescribed by AMLC.

d. There is an adequate and clear system of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregated amounts breach the threshold.

e. The ST reporting includes a reporting chain under which a suspicious transaction will be processed and a Board level or approved Committee is designated to ultimately decide whether or not the covered institution should file a report to the AMLC. If an Officer is designated to perform this function, the officer is identified and the process includes informing the Board of Directors of the Officer's decision.

3. Recordkeeping and retention policies and procedures

Covered institutions are required to maintain and safely store all customer identification records as long as the account exists. For closed accounts, retention period shall be limited to five (5) years from the date of closure. All transaction records, including all unusual or suspicious patterns of account activity is mandated by the rules to be maintained and safely stored for five (5) years from the date of transaction. In all instances, where a money laundering case is filed in court, all records shall be maintained and stored until the case has been finally resolved. In addition, Circular No. 706 directs covered institutions to designate at least two (2) officers who will be jointly responsible and accountable for the safekeeping of all these records and documents in such forms as are admissible in court.

4. Continuing education and training program

An effective training program includes provisions to ensure that:

a. All responsible officers and staff, including BOD and SM, who oversees, directs, manages, monitors, abides by or is involved in any way in the implementation of the MLPP or any customer transaction activity the AML system, shall receive appropriate training which includes awareness of their respective duties and responsibilities under the MLPP particularly in relation to the customer identification process, record keeping requirements and CT and ST reporting and ample understanding of the internal processes including the chain of command for the reporting and investigation of suspicious and money laundering activities. These officers and staff include but not limited to persons involved in branch administration, accounting, customer service, lending, private or personal banking, correspondent banking (international or domestic), trust, discount brokerage, fund transfer, safe deposit/custody and vault activities, record/bookkeepers, and IT personnel who maintains the AML system.

b. Training is designed to comprise of various focuses for new staff, front line staff, compliance staff, internal audit staff, officers, senior management, and

directors/stockholder. New and different money laundering schemes involving customers and financial institutions tailored to the audience, and the ways in which such activities can be detected or resolved should be addressed. It should also focus on the consequences of an employee's failure to comply with established policies and procedures (e.g., fines, suspension or termination). Programs should provide personnel with guidance and direction in terms of covered institution's policies and available resources as well as the safe harbor provisions protecting the personnel from lawsuits/administrative liabilities resulting from having made a CTR or STR in the regular performance of his duties and in good faith.

c. Regular refresher training is part of the program to inform responsible officers and staff of new developments and issuances related to the prevention of money laundering and terrorism financing as well as reminded of their respective responsibilities vis-à-vis the covered institution's processes, policies and procedures.

d. Training program and records of all ML and TF seminars and trainings conducted by the covered institution and/or attended by its personnel (internal or external), including copies of seminar/training materials, appropriately kept by the compliance office / unit / department, and made available during periodic or special BSP examination.

ANNEX B.1

SURVEY QUESTIONNAIRE[1]

A. MANAGEMENT

1. BOD and SM oversight

a. Is there a clear guidance from the BOD of the institution's strategic and operational plans and objectives in ensuring that the institution shall not be used as a ML and TF conduit? If so, please describe including the budget allocations to implement these plans and objectives. Have these plans and objectives been cascaded to Senior Management and responsible officers and staff? If so, state how this was done.

b. In relation to question no. 1, please describe the control policies and mechanisms (e.g. reportorial requirements, rewards and disciplinary system, training program, etc.) adopted by the BOD to attain these policies and objectives.

c. Please describe the institutional framework for ML and TF prevention. What are the roles of the BOD, Senior Management, Compliance Office, Internal Audit and other Offices in ML and TF prevention? What reports are required to be submitted to the BOD to assist them in their decision making processes?

d. Please describe the risk management system relative to ML and TF prevention.

e. Does the Compliance Office report directly to the BOD? If not, to whom does the Compliance office report? How frequent is this done?

f. Please describe the authorities delegated by the BOD to the Compliance Office and the AML Compliance Officer related to ML and TF prevention.

g. What other relevant oversight does the BOD and Senior Management exercise to ensure attainment of the institution's plans and objectives relative to ML and TF prevention?

2. Identification, measurement, monitoring and controlling or risks and problems related to ML and TF

a. Have you conducted risk profiling of all existing customers? If not all, what percentage of the total customer count had been profiled?

---

[1] *Responses in this survey questionnaire will provide the examiners with necessary information facilitating assessment of appropriate AML rating for the covered institution*

b. Have you conducted an assessment of the risks and vulnerabilities that your institution is exposed into? Please describe how the assessment was done.

c. What identified risks and vulnerabilities is the institution exposed into and how are these risks and vulnerabilities measured, monitored and controlled by the BOD and/or SM?

3. ***Self assessment systems that are either pro-active, through compliance testing, or reactive, through internal audit***

a. Have you conducted an over-all assessment of the institution's level of compliance with AMLA, as amended, its RIRR, and Circular No. 706? Please describe how this was done and state the frequency of the assessment.

b. Based on the assessment, please state in percentage the level of compliance of the institution.

c. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

d. Has your institution recently undergone an internal audit on AML Compliance? If yes, please summarize the key findings and/or recommendations that were noted in the most recent internal audit report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

Key Findings	Recommended Actions	Progress/Developments

e. Has your institution recently undertaken compliance testing of other departments, units, offices and branches that is independent of the internal audit? If yes, please describe the process (whether on-site inspections were conducted) and summarize the key findings and/or recommendations that were noted in the most recent compliance testing report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

Key Findings	Recommended Actions	Progress/Developments

4. Management Information System

a. Has the institution carried out an assessment of the effectiveness of the management information system as well as the AML electronic (for UBs/KBs) or manual (other institutions) monitoring system? Please specify how this is done.

b. What reports are being submitted to the BOD or Board level/approved Committee to assist them in their decision making processes relative to ML and TF prevention, who signs them and how frequent are they being required?

c. Does the institution keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? If so, which Office requires and maintains the same? Please provide copies of the statistics.

d. Does the institution keep track dispositions of red flag systems alerts? If so, which Office requires and maintains the same? Please provide copies of the tracking report.

5. Capability of Compliance Office in Managing the Institution's MLPP

a. Describe the structure of the Compliance Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualifications and experience as well as standards in hiring new staff, and control mechanisms (such as the power to monitor and ensure compliance including the authority to impose sanctions or give incentives or rewards when necessary) of the Office in ensuring that the pre-set objectives are adhered by responsible officers and staff in the different Departments, Groups, Units and/or Branches?

b. How are newly adopted policies and procedures as well as subsequent changes thereto assessed (as adequate or inadequate) and how are the results of the assessment communicated to the BOD to Senior Management, to different Departments, Units, Groups, Sub-groups and to the Branches up to the frontliners?

c. How is the adequacy of AML training assessed? Please specify in detail.

d. Have you taken the necessary measures to prevent criminals or their associates from holding or being the beneficial owners of a significant or controlling interest or holding a management function, including membership in the Board or any Committee within your financial institution? If yes, please describe the measures taken.

e. Do you have a screening process that ensure high standards when hiring employees? If yes, please indicate the specific policy provisions applicable.

f. Are the directors and senior management subject to internal "fit and proper" requirements including a check on their expertise and integrity? If yes, please provide the relevant policy provisions. If election, selection or appointment is based on family ties, please indicate.

g. Do you ensure that your foreign branches and subsidiaries observe AML/CFT measures consistent with the Philippine's legal requirements? If yes, please indicate the specific policy provisions.

h. In connection with the last question, was there an instance when the home country supervisor where a foreign branch or subsidiary is located has prohibited the branch or subsidiary from observing the Philippine laws, rules and regulations because it is prohibited by local (i.e. host country) laws, regulations or other measures? If yes, have you notified the BSP of this directive? Please indicate the specific legal provision(s) that provide(s) the legal basis for this requirement.

i. How are the provisions of the MLPP disseminated to responsible officers and staff and how are their compliance assessed and monitored?

j. What other relevant management practices does the Compliance Office exercise to manage its MLPP and ensure attainment of the institution's plans and objectives relative to ML and TF prevention?

6. ***Nature of weaknesses noted and ability to address existing and potential risks and problems***

a. Has your institution undergone a previous AML Examination by the BSP? If yes, please summarize the key findings and/or recommendations that were noted in the most recent AML report and set out the measures that the BOD has undertaken to address the findings and to monitor the same.

Key Findings	Recommended Actions	Progress/Developments

b. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

B. MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM

1. Customer identification process

a. Does the institution apply a risk based approach to combating money laundering and terrorist financing? If so, please provide an overview of these policies and procedures. The overview should (1) portray the institution's philosophy towards risk-based (does it form an integral part of the institution's business framework?), (2) indicate how the relevant risk assessments are undertaken and their bases to help determine the policy and its practical application, and (3) describe the mechanism by which permitted variations from the generally applicable standards are promulgated, and what arrangements, if any, are in place to monitor the continuing suitability of the exceptions. Please provide the basis in the institution's MLPP.

b. Does your institution permit the opening of anonymous accounts, accounts in fictitious names and other accounts not otherwise under the true and full name of the accountholder? If yes, please indicate the approximate number of accounts, pertinent policies and procedures for opening and the level of approving authority.

c. Are numbered accounts permitted? If yes, describe the existing framework governing them such as but not limited to the identification of the Office responsible for maintaining them, the approving authority, the procedures, requirements and control mechanisms for the opening, maintaining and monitoring of these accounts, and the frequency for updating KYC information.

d. Does your institution undertake customer due diligence (CDD) measures when:

1) establishing business relations?
2) carrying out transactions with non-clients?
3) carrying out occasional transactions such as purchase of manager's/cashier's checks and of acquired assets whether in cash or installments, purchase and sale of foreign currency notes, acceptance of second-endorsed checks?
4) carrying out and receiving wire, domestic or cross border, transfers?
5) dealing with trustee, nominee, agent, or intermediary, applying CDD not only on the latter but also on the trustors or principals?
6) dealing with juridical entities that have no business substance in their own right but through which financial transactions may be conducted, applying CDD on the entities' beneficial owner?
7) the financial institution has doubts about the veracity of previously obtained customer identification document or data?
8) transacting directly or indirectly with a numbered accountholder?

For each of the above, please describe in detail the CDD process and the specific provision in the MLPP that apply.

e. Explain the CDD requirements applicable to potential individual customers stating the minimum information to be obtained, IDs acceptable and its classification based on reliability (if any), and policy in updating identification information citing the specific internal policy provisions.

f. Explain the CDD requirements applicable to potential customers that are juridical entities and the persons acting on their behalf such as but not limited to the President and the authorized signatory/ies stating the minimum information to be obtained, IDs acceptable and its classification based on reliability (if any), measures to prevent the unlawful use of legal persons in relation to money laundering and terrorist financing and policy in updating identification information citing the specific internal policy provisions.

g. Does your institution identify the beneficial owner of juridical entities dealing with the institution and verify the information acquired? If yes, please describe in detail including the specific internal policy provisions.

h. Does your institution conduct ongoing due diligence on the business relationship of existing customers? If yes, please describe the extent/scope of this obligation and indicate the specific internal policy provisions.

i. Does your institution perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and does it apply to existing customers? If yes, please explain including reference to the list of customers considered as high risk, criteria and factors considered in applying EDD, types of measures required, control mechanisms for managing the risks associated with dealing with these customers, validation procedures and the specific internal policy provisions.

j. Does your institution apply reduced due diligence where there is low risk of ML or TF? If yes, please explain providing details of any applicable conditions/standards and specific internal policy provisions. Is this permitted with regard to customers that are resident in another country? If yes, please explain further.

k. What does your institution do in cases where it is unable to complete the CDD measures required by existing internal rules or under the UARR, the AMLA, as amended, and its RIRR? Please indicate the specific internal policy provisions that apply.

l. What are your obligations with regard to establishing business relationships with a politically exposed person, his/her relative, entities related to them? Please describe

the existing policies governing these arrangements, including the standard of due diligence that apply to them on account opening, control mechanisms to address the risks associated with dealing with them, and updating of identification information with references to specific internal policy provisions.

m. In relation to cross-border correspondent banking, are the following required by internal rules?

- Understand fully the nature of the correspondent's business?
- Determine from publicly available information the reputation of the institution and the quality of supervision?
- Determine whether it has been subject to a money laundering or terrorist financing investigation or regulatory action?
- Assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective?
- Obtain approval from senior management before establishing new correspondent relationships?
- Clarify the respective AML/CFT responsibilities of each institution in a written document?

Please indicate the specific internal policy provisions that apply to each of the above.

n. Where a correspondent relationship involves the maintenance of "payable-through accounts", are you required to be satisfied that:

(1) your customer (the respondent financial institution) has verified the identity of, and performed on-going due diligence on, the customers that have direct access to the accounts of the correspondent financial institution; and

(2) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution?

Please provide the specific internal policy provisions that apply for each of the above.

o. What policies are in place where your institution is the originating, intermediary or beneficial institution? Please explain in detail including the obligations of the institution in case the fund transfer is not accompanied with originator information citing specific internal policy provisions.

p. When acting as a beneficiary institution in a fund/wire transfer, are you required to do the following by your internal rules?

- Conduct CDD on the beneficiary before paying out the transfer
- Conduct CDD on the ordering financial institution
- Require originator information (if yes, please specify what kind of originator information do you require: name of the originator, address, national identity number, date and place of birth of the originator, account number of the originator, or a unique reference number) to be attached in the transfer message when the transfer, both domestic and cross-border, amounts to P50,000 or more or its equivalent
- Apply enhanced due diligence on the beneficiary and the originator when the originator is a high risk customer by its own standards
- Exert efforts to establish the true and full identity and existence of the originator by requiring additional information from the originator institution or intermediary institution when the transfer amounting to P50,000 or more is unaccompanied by originator information
- Apply enhanced due diligence to establish the true and full identity and existence of the beneficiary when the transfer amounting to P50,000 or more is unaccompanied by originator information
- Refuse to effect the transfer or the pay-out of funds where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory when the transfer amounting to P50,000 or more is unaccompanied by originator information

Please provide the specific internal policy provisions for each of the above. In case of the last item, explain how the transfer fund is treated by the institution (whether frozen or immediately returned to the originator) stating the specific internal policy provision that apply.

q. Does your institution allow non-face-to-face services (transactions with trustee, nominee, agent or intermediary accounts including account opening)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

r. Do any of your businesses make use of third parties, referral by Brokers, intermediaries, fiduciaries, affiliates, subsidiaries and the like (Collectively called as third parties)? If Yes, please identify the third-parties and the due diligence undertaken on the third parties. Please also identify the business areas which make use of third parties, the approval process for introducing clients, the type of relationship, and whether or not such third parties perform the CDD process that would usually be undertaken by the institution;

s. Do you rely on third parties to perform some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

t. Are there instances where you outsource some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

u. Does your institution offer private banking/ wealth management or similar activities? If yes, please describe the existing policies governing these arrangements, including the standard of due diligence that apply to them, level of authority of the relationship officers (or similar officers handling the account or relationship), the approving officers for establishing business relationships or effecting the transactions, control mechanisms to address the risks associated with dealing with the business relationship, and updating of identification information with references to specific internal policy provisions.

v. What standard of due diligence do you apply when establishing business relationships with foreign exchange dealers, money changers remittance agents, and shell companies? Please explain the existing policies and procedures for customer acceptance that apply to them (including whether or not you require that they register with the BSP before dealing with them), control mechanisms to address the risks associated with dealing with them (including continuous monitoring of their transactions), and updating of identification information with references to specific internal policy provisions.

w. What are your obligations with regard to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations? Please provide the internal policy provisions which serve as basis for these obligations.

x. Are there measures in place to ensure that your institution is advised of concerns about weaknesses in the AML/CFT systems of other countries? If yes, please describe these measures and how these concerns are incorporated into the institution's Program.

y. Are there measures in place to ensure that funds or other assets collected by or transferred through non-profit organizations are not diverted to support the activities of terrorists or terrorist organizations? If so, please specify what these measures are and indicate the specific policy provisions.

2. Record keeping and retention process

a. Please describe the record-keeping obligation including the type of records and information that should be maintained. Please indicate the specific internal policy provisions.

b. Do you maintain all necessary records on transactions, both domestic and international and, if so, for how long following completion of the transaction? Who are the two (2) designated custodian that shall be accountable and responsible for safekeeping these documents?

c. Do you maintain records of the identification documents and data, account files and business correspondence and, if so, for how long following the termination of an account or business relationship?

d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the the two (2) designated custodian that shall be accountable and responsible for safekeeping and making these records available with references to specific internal policy provisions.

3. Covered and Suspicious Transaction Reporting

a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

- Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
- Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
- Investigation – checks for given names throughout the history of payment stored in the system;
- Can generate all the CTRs of the covered institution accurately and completely with all the mandatory field properly filled up;
- Must provide a complete audit trail;
- Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
- Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC.

b. If no, please describe how you manually perform the functionalities mentioned above.

c. Do you pay special attention to unusual transactions? If yes, how do you define unusual transactions? And what type of special measures do you implement in managing them? Please indicate the specific internal policy provisions for this requirement.

d. Are you required to report to the AMLC a suspicious transaction report – STR, when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the institution (whether or not to file an STR) with references to the specific internal policy provisions that mandate reporting.

e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the institution (whether or not to file an STR) with reference to the specific internal policy provisions that mandate reporting.

f. Other than the 6 specified circumstances for filing an STR, what other instances do you report an STR or an alert has been tagged using the last item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report? Please describe, by reference to the specific internal policy provisions, the scope of the protection in terms of who would benefit from it and the types of liability against which it is available.

h. Do you prohibit your officers and staff from disclosing ("tipping off") to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC? If they are, please describe the scope of this prohibition by reference to the specific internal policy provisions.

4. ***Employment and Training Program***

a. Please indicate the standards that apply when hiring new staff to the Compliance Office, the Internal Audit and the institution as a whole?

b. Please describe the institution's AML training and refresher program with specific references to the level of training and focus on the participant, the Office tasked to

implement the program, the financial, human and technical support that that Office has been given and frequency of offering.

c. Are the staff of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices? Please give details.

d. Do you have an on-going employee training on AML/CFT? If yes, please indicate the last employee training on AML/CFT and the schedule for the year as well as the specific policy provisions for this requirement.

C. CONTROLS AND AUDIT

a. What is the structure of the Internal Audit Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualification and experiences as well as standards in hiring new staff, and control mechanisms of the Office in ensuring that the pre-set objectives are adhered by responsible officers and staff in the different Department, Groups, Units and/or Branches?

b. Do you establish and maintain internal procedures, policies and controls to prevent ML and TF? How do you communicate these to the officer, staff and employees? Please provide details with reference to the applicable policy provisions.

c. Do you maintain an adequately resourced and independent audit function that tests compliance with these procedures, policies and controls? If yes, please indicate the available resources, financial, human, and technical and the specific policy provisions for this requirement.

D. IMPLEMENTATION

1. Covered and Suspicious Transaction Reporting Policies and Procedures

a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

- Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
- Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;

- Investigation – checks for given names throughout the history of payment stored in the system;
- Can generate all the CTRs of the covered institution accurately and completely with all the mandatory field properly filled up;
- Must provide a complete audit trail;
- Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
- Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC.

b. If no, please describe how you manually perform the functionalities mentioned above.

c. Do you pay special attention to unusual transactions? What type of special measures do you implement in managing them?

d. Are you required to report to the AMLC a suspicious transaction report – STR, when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the institution (whether or not to file an STR).

e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the institution.

f. Other than the 6 specified circumstances for filing an STR, what other instances do you report an STR or an alert has been tagged using the last item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report?

h. Does the Compliance Office keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? Please provide copies of the statistics.

i. Does the Compliance Office keep track dispositions of red flag systems alerts? Please provide copies of the tracking report.

j. Do you prohibit your officers and staff from disclosing ("tipping off") to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC?

2. ***Risk based and tiered customer acceptance, identification and on-going monitoring policies and procedures***

   a. Does your institution undertake customer due diligence (CDD) measures when:
      (1) establishing business relations?
      (2) carrying out transactions with non-clients?
      (3) carrying out occasional transactions such as purchase of manager's/cashier's checks and of acquired assets whether in cash or installments, purchase and sale of foreign currency notes, acceptance of second-endorsed checks?
      (4) carrying out and receiving wire, domestic or cross border, transfers?
      (5) dealing with trustee, nominee, agent, or intermediary, applying CDD not only on the latter but also on the trustors or principals?
      (6) dealing with juridical entities that have no business substance in their own right but through which financial transactions may be conducted, applying CDD on the entities' beneficial owner?
      (7) the financial institution has doubts about the veracity of previously obtained customer identification document or data?
      (8) transacting directly or indirectly with a numbered accountholder?

   b. Does your institution identify the beneficial owner of juridical entities dealing with the institution and verify the information acquired?

   c. Does your institution conduct ongoing due diligence on the business relationship of existing customers?

   d. Does your institution perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and does it apply to existing customers?

   e. Does your institution apply reduced due diligence where there is low risk of ML or TF? What does your institution do in cases where it is unable to complete the CDD measures required by existing internal rules or under the UARR, the AMLA, as amended, and its RIRR?

   f. What does your institution do in cases where it is unable to complete the CDD measures required by existing internal rules or under the UARR, the AMLA, as amended, and its RIRR?

   g. Where a correspondent relationship involves the maintenance of "payable-through accounts", are you required to be satisfied that:

      (1) your customer (the respondent financial institution) has verified the identity of, and performed on-going due diligence on, the customers that have direct access to the accounts of the correspondent financial institution; and

(2) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution?

h. When acting as a beneficiary institution in a fund/wire transfer, are you required to do the following by your internal rules?

- Conduct CDD on the beneficiary before paying out the transfer
- Conduct CDD on the ordering financial institution
- Require originator information (if yes, please specify what kind of originator information do you require: name of the originator, address, national identity number, date and place of birth of the originator, account number of the originator, or a unique reference number) to be attached in the transfer message when the transfer, both domestic and cross-border, amounts to P50,000 or more or its equivalent
- Apply enhanced due diligence on the beneficiary and the originator when the originator is a high risk customer by its own standards
- Exert efforts to establish the true and full identity and existence of the originator by requiring additional information from the originator institution or intermediary institution when the transfer amounting to P50,000 or more is unaccompanied by originator information
- Apply enhanced due diligence to establish the true and full identity and existence of the beneficiary when the transfer amounting to P50,000 or more is unaccompanied by originator information
- Refuse to effect the transfer or the pay-out of funds where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory when the transfer amounting to P50,000 or more is unaccompanied by originator information

i. In case of non-face-to-face services, does the Bank ensure that control measures to address risks associated with this type of business relationships or transactions are implemented?

3. Record-keeping and retention policies and procedures

a. What are the type of records and information that your institution maintains?

b. Do you maintain all necessary records on transactions, both domestic and international and, if so, for how long following completion of the transaction? Who are the two (2) designated custodian that shall be accountable and responsible for safekeeping these documents?

c. Do you maintain records of the identification documents and data, account files and business correspondence and, if so, for how long following the termination of an account or business relationship?

d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the the two (2) designated custodian that shall be accountable and responsible for safekeeping and making these records available.

e. Do you conduct compliance testing to ensure that all units and/or branches maintain and safely store KYC and transaction records?

f. Does the Internal Audit cover an assessment of compliance of the record-keeping and retention process?

4. Continuing education and training program

a. Are newly-hired employees required to attend AML training?

b. Is there an existing training and refresher program for all responsible officers and staff? Please a copy of the program.

c. Are the staffs of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices?

d. Do you have an on-going employee training on ML and TF prevention? If yes, please indicate the last employee training and the schedule for the year.

e. Do you conduct a regular post-test on employees to gauge their understanding of AMLA, as amended, its RIRR and Circular No. 706?

ANNEX C

MONETARY PENALTY GUIDELINES

These guidelines are divided into three (3) parts. Part I is the monetary penalty matrixes, where monetary penalties are categorized based on the (1) Composite rating and (2) Asset size of the BSP covered institution. Part II presents the guiding principles in determining the amount of penalty including the steps in identifying the proper amount of penalty. Lastly, Part III shows the aggravating and mitigating factors that may be considered in determining whether to impose the penalty in the maximum, medium or minimum range.

PART I

PENALTY MATRIX A (To be used when a BSP covered institution's Composite rating is **"1"**)

	Up to P100 Million	Above P100 Million but not exceeding P500 Million	Above P500 Million but not exceeding P5 Billion	Above P5 Billion but not exceeding P50 Billion	Above P50 Billion
Minimum	P 5,000	P 10,000	P 15,000	P 20,000	P 25,000
Medium	7,500	12,500	17,500	22,500	27,500
Maximum	10,000	15,000	20,000	25,000	30,000

PENALTY MATRIX B (To be used when a BSP covered institution's Composite rating is **"2"**)

	Up to P100 Million	Above P100 Million but not exceeding P500 Million	Above P500 Million but not exceeding P5 Billion	Above P5 Billion but not exceeding P50 Billion	Above P50 Billion
Minimum	P 3,000	P 5,000	P 10,000	P15,000	P 15,000
Medium	4,000	7,500	12,500	17,500	17,500
Maximum	5,000	10,000	15,000	20,000	20,000

PART II- Guiding Principles

1. The first step is to determine the over-all risk rating of the BSP covered institution for purposes of identifying which penalty matrix will be used. If the Composite rating is **"1"**, or **"2"**, penalty matrix A or B, respectively shall be used. If the over-all rating is **"3"** and **"4"**, no monetary penalty shall be imposed.

2. Second step is to establish the asset size of the BSP Covered institution as of the cut-off period of examination;

3. Third step is to identify the aggravating and mitigating factors. If the aggravating factors are more than the mitigating factors, then the maximum range shall be used. On the other hand, if the mitigating factors are more than the aggravating factors, then the minimum range shall be applied. In case there are no aggravating and mitigating factors or there is a tie, the medium range shall be used.

4. For Composite ratings of 1 and 2 where the covered institution concerned was required to submit within a reasonable period of time an acceptable plan, non-submission of the plan within the deadline or failure to implement the action plan shall be a basis for imposition of monetary penalties computed on a daily and continuing basis from the time the covered institution is notified until corrective measures are satisfactorily effected. The penalty may be imposed on the covered institution itself or directly on the Board of Directors as a body, or the individual directors who have direct oversight, or the line officers involved in the management of money laundering and terrorist financing prevention.

PART III- Aggravating and Mitigating Factors

A. Aggravating Factors

a. Frequency of the commissions or omissions of specific violation- Majority of the following violations were noted:

1. Deficient Know Your Customer process
2. Unsatisfactory Covered Transaction reporting system
3. Non-reporting of and improper Suspicious Transaction reporting
4. Non-compliance with the Record keeping requirement
5. Inadequate AML Training Program
6. Deficient AML Electronic system

b. Duration of violations prior to notification- This pertains to the length of time prior to the latest notification on the violation. Violations that have been existing for a long time before it was revealed/discovered in the examination or are under evaluation for a long time due to pending requests or correspondences from covered institutions on whether a violation has

actually occurred shall be dealt with through this criterion. Violations outstanding form more than one (1) year prior to notification, at the minimum, will qualify as violations outstanding for a long time.

c. Continuation of offense or omission after notification- This pertains to the persistence of an act or omission after the latest notification on the existence of the violation, either from the appropriate SES Group, Department or from the Monetary Board and/or Deputy Governor, in cases where the violation has been elevated accordingly. This covers the period after the final notification of the existence of the violation until such time that the violation has been corrected and/or remedied. The corrective action shall be reckoned with from the date of notification.

d. Concealment- This factor pertains to the cover up of a violation. In evaluating this factor, one shall consider the intention of the party/ies involved and whether pecuniary benefit may accrue accordingly. The act of concealing an act or omission constituting the violation carries with it the intention to defraud regulators. Moreover, the amount of pecuniary benefit, which may or may not accrue from the offense or omission, shall also be considered under this factor.

Concealment may be apparent when a covered institution's personnel purposely complicate the transaction to make it difficult to uncover or refuse to provide information and/or document that would support the violation/offense committed.

e. Loss or risk of loss to bank- In asserting this factor, "potential loss" refers to any time at which the covered institution was in danger of sustaining a loss.

B. Mitigating Factors

a. Good Faith is the absence of intention to violate on the part of the erring individual/entity.

b. Full cooperation- covered institution's personnel or the covered institution immediately took action to correct the violation after it is brought to its attention either verbally or in writing.

c. With positive measures- covered institution's personnel or the covered institution commits to undertake concrete action to correct the violation but is being restrained by valid reasons to take immediate action.

d. Voluntary disclosure of offense- covered institution's personnel or the covered institution disclosed the violation before it is discovered in the course of a regular or special examination or off-site monitoring.